

[UNIX] Witango & Tango 2000 Application Server Remote System Buffer Overrun

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0079.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/20/03

To: list@securiteam.com

Date: 20 Jul 2003 20:43:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Witango & Tango 2000 Application Server Remote System Buffer Overrun

SUMMARY

As detailed on <<http://www.witango.com>> <http://www.witango.com> – Witango can "provide your Web Application with a solid application framework, a simple interface for both the production and ongoing maintenance of complex application logic, a variety of mechanisms to integrate to non-web interfaces, and a wide range of database connectivity options. The Witango product suite provides a comprehensive Integrated Development Environment (IDE) to enable application developers to rapidly generate XML files that can then be deployed to a wide range of operating systems. Witango is a fast to learn, easy to use, scalable solution for the Professional Web Application Developer".

A buffer overflow in the cookie buffer allows a buffer overrun and remote exploit.

DETAILS

Securiteam: [UNIX] Witango & Tango 2000 Application Server Remote System Buffer Overrun

Vulnerable systems:

* All Tango 2000 versions, Witango under 5.0.1.062

Immune systems:

* Witango 5.0.1.062

By passing a long cookie to Witango_UserReference we overwrite the saved return address on the stack. As Witango is installed as LocalSystem, any arbitrary code execution will run as SYSTEM

GET /ngssoftware.tml HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*

Accept-Language: en-gb

User-Agent: My Browser

Host: ngssoftware.com

Connection: Keep-Alive

Cookie: Witango_UserReference= parameter length 2864

Vendor Status:

Mark has been asked by Phil Wade of Witango to mention the following: "We also did some tests on older versions of the server and found the vulnerability also exists in the previous version of the server which was known as Tango 2000. Can you also mention that Tango 2000 is also vulnerable and should be upgraded to Witango 5.0.1.062 especially if the Tango 2000 server is accessible from the internet".

ADDITIONAL INFORMATION

Information supplied by <<mailto:mark@ngssoftware.com>> Mark Litchfield

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.